DOSSIER SOLUTION
RGPD de l'UE

Conformité RGPD : comment s'adapter à la nouvelle réglementation ?

ca technologies

Depuis plus de vingt ans, les entreprises doivent se conformer à différentes directives et réglementations en matière de protection des données. Le Règlement général sur la protection des données (RGPD ou GDPR en anglais), qui reprend l'ensemble des législations existantes de la Commission européenne en matière de protection des données, a toutefois pour but de renforcer et d'harmoniser ces différentes réglementations pour les citoyens européens. Les principaux objectifs du RGPD sont de redonner aux citoyens un contrôle sur leurs données personnelles et de simplifier le cadre réglementaire pour les entreprises internationales. Pour les organisations déjà conformes à la Directive 95/46/CE, quels sont les critères technologiques à remplir pour garantir la conformité au RGPD ?

Section 1 :

Présentation du Règlement général sur la protection des données (RGPD)

À partir du 25 mai 2018, toute organisation traitant les données personnelles de citoyens de l'Union européenne devra impérativement être conforme au RGPD. Cette réglementation introduit de nouvelles exigences en matière de protection des données, qui affecteront la majorité des entreprises, quel que soit leur secteur d'activité. Toute organisation qui ne respecterait pas les exigences du RGPD pourra se voir appliquer une amende administrative allant jusqu'à 20 000 000 € ou jusqu'à 4 % de son chiffre d'affaires mondial, au plus élevé des deux.

Outre la volonté de renforcer la protection des données, le RGPD a également pour but d'harmoniser les différentes lois sur la protection de la vie privée appliquées au sein de l'Union européenne (UE), ce qui devrait, dans une certaine mesure, aider les entreprises à normaliser leurs règles et processus en la matière.

Le tableau ci-dessous répertorie les exigences du RGPD en différentes catégories de haut niveau :

Catégorie	Exigences
Droits des personnes concernées	1. Les personnes concernées (voir définition n° 1) doivent pouvoir : a. Accéder à leurs données. b. Rectifier et supprimer (droit à l'oubli) leurs données, et en restreindre l'utilisation (voir définition n° 2). c. Bénéficier d'une portabilité de leurs données. d. Refuser l'utilisation de leurs données.
Responsabilité	2. Les organisations qui traitent des données personnelles doivent : a. Mettre en place les mesures techniques et organisationnelles appropriées pour garantir et prouver que le traitement des données s'effectue dans le respect du RGPD. b. Obtenir le consentement de la personne concernée pour certaines activités de traitement. c. Mettre en œuvre des politiques et des processus de protection des données adéquats. d. Conserver une trace de toutes les activités de traitement. e. Informer l'autorité de contrôle dans certains cas de violations de données personnelles. f. Informer la personne concernée dans certains cas de violations de données personnelles. g. Désigner un délégué à la protection des données (DPD), lorsque cela est nécessaire.
Protection des données dès la conception et par défaut	3. Mise en œuvre de mesures techniques et organisationnelles appropriées : a. Qui sont conçues pour appliquer différents principes de protection des données, telles que la pseudonymisation et la minimisation des données, de façon effective et pour assortir le traitement des garanties nécessaires. b. Qui, par défaut, ne rendent pas les données personnelles accessibles à un nombre indéfini de personnes physiques sans intervention de la personne concernée.
Signalement des violations de données	4. En cas de violation de données à caractère personnel (voir définition n° 7) : a. Les responsables du traitement doivent notifier la violation en question à l'autorité de contrôle compétente, 72 heures au plus tard après en avoir pris connaissance. b. Les sous-traitants (voir définition n° 8) notifient au responsable du traitement toute violation dans les meilleurs délais après en avoir pris connaissance. c. Ils communiquent à la personne concernée la violation de ses données à caractère personnel (sauf exceptions).

Catégorie	Exigences
Anonymisation et pseudonymisation	5. Des techniques de pseudonymisation et d'anonymisation doivent être appliquées : a. Dans le cadre du principe de « protection des données dès la conception et par défaut », lors du traitement de données à caractère personnel. b. Pour les données archivées dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.
Transferts de données transfrontaliers et règles d'entreprise contraignantes	6. Les données à caractère personnel sont soumises aux restrictions suivantes en matière de transfert : a. Vers les pays extérieurs à l'Espace économique européen considérés comme « non adéquats ». b. Les règles d'entreprise contraignantes (voir définition n° 9) et les clauses contractuelles standard (ou clauses types) établies par la Commission européenne restent des instruments valides pour garantir la conformité aux restrictions de transfert de données en provenance de l'UE (voir définition n° 10). c. Bouclier de protection des données (voir définition n° 11).
Certifications, codes de conduite et labels	7. Les organisations auront la possibilité d'adopter des mécanismes de certification aux fins de démontrer l'existence et la conformité de certaines garanties qu'ils appliquent.

Les définitions proviennent du texte du RGPD.

1. **Personne concernée :** « personne physique identifiable », c'est-à-dire une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
2. **Limitation du traitement :** marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.
3. **Responsable du traitement :** personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.
4. **Autorité de contrôle :** autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51.
5. **Délégué à la protection des données :** le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.
6. **Pseudonymisation :** traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.
7. **Violation de données à caractère personnel :** violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

8. **Sous-traitant :** personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

9. **Règles d'entreprise contraignantes :** règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe.

Autres définitions pertinentes dans le cadre du RGPD

10. **Pays adéquats :** les données à caractère personnel peuvent être transférées des 28 États membres de l'UE et de trois États membres de l'EEE (Norvège, Liechtenstein et Islande), vers le pays tiers concerné sans qu'il soit nécessaire de prévoir d'autres garanties.

    La Commission a constaté à ce jour **qu'Andorre, l'Argentine, le Canada** (organisations commerciales), **les Îles Féroé, Guernesey, Israël, l'Île de Man, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay** prévoient une protection adéquate. (voir http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (en anglais))

11. Pour transférer des données à caractère personnel de l'UE vers les États-Unis, différents outils sont disponibles, notamment des clauses contractuelles, des règles d'entreprise contraignantes et le « bouclier de protection des données ». Dans le cas du bouclier de protection des données, les entreprises américaines concernées doivent tout d'abord signer ce cadre réglementaire auprès du ministère du Commerce des États-Unis. Les obligations imposées aux entreprises au titre du bouclier de protection des données sont présentées dans la section « Principes de la sphère de sécurité ». Il est de la responsabilité du ministère du Commerce de gérer et d'administrer le bouclier de protection des données et de garantir que les entreprises qui y adhèrent respectent leurs engagements au titre de celui-ci. Pour pouvoir obtenir une certification, les entreprises doivent avoir mis en place une politique en matière de protection de la vie privée qui soit conforme aux principes de la sphère de sécurité. Elles doivent également renouveler chaque année leur « autocertification » au titre du bouclier de protection des données. Dans le cas contraire, elles ne pourront plus recevoir ni utiliser de données à caractère personnel en provenance de l'Union européenne, dans ce cadre précis. Une liste des entreprises autocertifiées dans le cadre du bouclier de protection des données est disponible sur le site Web du ministère du Commerce des États-Unis (https://www.privacyshield.gov/welcome). Le site présente également une liste des entreprises ayant perdu leur certification au bouclier de protection des données.

Section 2 :

Exigences

Droits des personnes concernées

Il s'agit de l'un des thèmes les plus importants de cette réglementation. Les critères ont été revus à la hausse et de nouveaux droits ont été inclus, lesquels affecteront de façon radicale la manière dont les organisations IT devront traiter et contrôler les données personnelles. Il est important de comprendre que le RGPD a été créé en remplacement de la **Directive relative à la protection des données** (Directive 95/46/CE) et que son objectif est de renforcer et d'unifier la protection des données pour les citoyens de l'Union européenne.

Alors que les droits traditionnels d'accès (art. 15), de rectification (art. 16), d'effacement (art. 17) et d'opposition (art. 21) restent sensiblement les mêmes, un nouveau droit fait son apparition : le droit à la portabilité des données (art. 20) ; par ailleurs, des modifications ont été apportées au droit à l'effacement en incluant le concept de « droit à l'oubli » (art. 17) et en ajoutant le droit à la limitation du traitement (art. 18). Ces droits sont désormais fondamentaux et universels au sein de l'UE, alors que dans le cadre de la précédente directive, chaque État membre était autorisé à les interpréter à sa guise, ce qui compliquait grandement la tâche lorsque les personnes concernées tentaient de faire valoir leurs droits.

Les organisations doivent relever de multiples défis et certains des nouveaux droits, notamment celui de la portabilité des données, qui permet à des individus d'obtenir et de réutiliser leurs données personnelles pour leurs propres fins entre différents services, sont probablement l'un de ces défis les plus importants. Il est donc aujourd'hui nécessaire d'adopter un modèle qui aide les entreprises à couvrir les besoins actuels et futurs.

Pour que les applications existantes qui intègrent des données à caractère personnel puissent devenir compatibles avec cette nouvelle réglementation, tout en évitant le coût élevé lié à des modifications, une seule réponse s'impose : les API.

L'adoption d'un modèle basé sur des API pour l'accès aux données est le fondement d'une architecture évolutive, qui permettra à l'entreprise de se mettre en conformité vis-à-vis de cette réglementation et de celles qui suivront. En effet, les API peuvent être sécurisées, gouvernées et améliorées par l'implémentation de solutions logicielles appropriées.

Le RGPD renforce également l'exigence d'obtenir le consentement de la personne concernée. Les organisations devront donc gérer leur relation avec la personne concernée d'une manière différente. Les identités numériques et la gestion, la gouvernance et le contrôle d'accès associés joueront un rôle important pour ceux qui souhaitent se conformer avec succès à cette nouvelle réglementation.

Pour garantir le respect du RGPD, les organisations devront adopter de nouveaux canaux de communication avec les personnes concernées, de façon à s'assurer qu'elles sont en mesure d'exercer correctement leurs droits fondamentaux. Il sera donc nécessaire d'appliquer des mesures techniques pour permettre un accès sécurisé et adéquat des individus à leurs données. De nouveaux canaux devront également être créés afin que les personnes concernées puissent exercer leur droit de portabilité des données et lancer le processus de transfert de leurs propres données vers le tiers désigné. Il est donc impératif de déployer des contrôles d'accès solides et une sécurité adaptée pour ces nouvelles passerelles de données.

Bien que cela puisse sembler simple, les données personnelles peuvent être accessibles sur de nombreux serveurs et systèmes de fichiers ; il est donc essentiel d'appliquer aux infrastructures IT des mécanismes de détection, d'analyse et de classification appropriés avant même de mettre en œuvre des règles de protection des données.

Responsabilité

La nouvelle réglementation est parsemée d'exigences techniques, mais ce qui en ressort est le principe de « responsabilité » pour les responsables du traitement des données et/ou les sous-traitants. En d'autres termes, lorsqu'un incident se produit, ce qui est quasiment inévitable, l'organisme de réglementation recherchera la preuve que l'entreprise faisant l'objet de l'enquête a bien appliqué tous les contrôles techniques et organisationnels nécessaires pour garantir le traitement approprié des données à caractères personnel, conformément au RGPD. L'entreprise doit quant à elle prouver qu'elle a mis en place les mesures et contrôles IT requis par le règlement, et effectuer une supervision et un reporting continus de toutes les actions entreprises. Son incapacité à prouver ces démarches déterminera grandement le montant de l'amende administrative, le cas échéant. Ces éléments sont clairement établis dans l'article 83.

Dans le monde IT hybride actuel, il n'est malheureusement pas toujours simple de déterminer, au sein des systèmes, quelles données appartiennent à qui. Cela peut constituer un vrai problème pour les organisations, qui devront rechercher et détecter les données à caractère personnel sur les plates-formes existantes les plus variées. Elles devront en outre mettre en œuvre des solutions logicielles pour les aider, non seulement à identifier les informations, mais également à les contrôler et à suivre l'usage de ces données personnelles sur l'ensemble de leur cycle de vie. L'incapacité à implémenter des contrôles techniques matures dans ce domaine jouera certainement en défaveur de l'organisation en cas d'incident.

Protection des données dès la conception et par défaut

L'article 25, paragraphe 2, stipule que « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. » L'article 30 impose quant à lui la tenue d'un registre des activités de traitement.

L'article 32, « Sécurité du traitement », dans sa section 1(b), exige « des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ». La section 1(d) impose la mise en œuvre d'« une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ».

Il s'agit là d'un sujet très large qui exige une approche holistique incluant différents processus de développement logiciel, notamment des tests, des Q&R et le lancement de nouvelles versions. Toutes ces disciplines IT exigent une couche intégrée de contrôles de sécurité afin de garantir que les données sont accessibles uniquement par les personnes appropriées et aux fins pour lesquelles elles ont été recueillies au départ.

Signalement des violations de données

Dans la suite du principe de responsabilité expliqué ci-avant, les responsables du traitement des données et les sous-traitants sont tenus de signaler certaines violations de données affectant les données à caractère personnel. Les types de violation imposant une notification sont décrits dans les articles 33 et 34.

L'article 33 établit l'obligation de notifier les violations de données à l'autorité de contrôle compétente et l'article 34 établit la même obligation, mais envers la personne concernée. Il est important de noter que, conformément à l'article 34.3, l'organisation est dispensée de notifier l'incident à la personne concernée dans les cas suivants :

- Le responsable du traitement **a mis en œuvre les mesures de protection techniques et organisationnelles appropriées** et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement.
- Le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser.

La notification de la violation de données au responsable du traitement par un sous-traitant doit avoir lieu dans les plus brefs délais, et la notification du responsable du traitement à l'autorité de contrôle compétente au plus tard dans les 72 heures après avoir pris connaissance de l'incident. Le rapport de notification doit indiquer précisément les tenants et les aboutissants de la violation (qui, quand, quoi), ainsi que les actions et mesures mises en œuvre pour en atténuer les effets négatifs potentiels.

Anonymisation et pseudonymisation

Le RGPD introduit de nouveaux concepts relatifs aux principes à appliquer dans la gestion et le traitement des données à caractère personnel. Protéger les données à caractère personnel et redonner le contrôle de celles-ci aux personnes concernées est le principal objectif de ce règlement, qui présente donc différentes techniques de protection des données personnelles.

Le chapitre II (« Principes ») illustre l'intention de renforcer la façon dont les données à caractère personnel sont traitées (« minimisation des données ») et conservées sous une forme ne permettant pas d'identifier plus longtemps que nécessaire la personne concernée. D'autre part, le traitement des données à caractère personnel doit s'effectuer de manière à garantir une sécurité adéquate, notamment en offrant une protection contre tout traitement non autorisé ou illicite et toute perte, destruction ou altération accidentelle, à l'aide de mesures techniques et organisationnelles adaptées (« intégrité et confidentialité »).

Transferts de données transfrontaliers et règles d'entreprise contraignantes

Tout comme dans la précédente directive, l'article 45 du règlement établit des restrictions sur les transferts internationaux de données à caractère personnel, vers des pays « non adéquats » situés à l'extérieur de l'Union européenne. L'article 46, paragraphe 2, établit les garanties appropriées pouvant être fournies sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle.

Les règles d'entreprise contraignantes (art. 47) et les clauses contractuelles standard (ou clauses types) établies par la Commission européenne restent des instruments valides pour garantir la conformité aux restrictions de transfert des données provenant de l'UE. Il devrait devenir plus facile d'utiliser ces mécanismes pour les transferts intra-groupe, car certaines exigences d'autorisation ont été abandonnées. Consultez pour cela les définitions 10 et 11 relatives aux implications pour le bouclier de protection des données aux États-Unis.

Contrôler qui a accès aux données est une étape fondamentale pour respecter cette exigence. Les organisations devront effectuer des campagnes de certification d'accès périodiques afin de s'assurer que les droits d'accès de leurs utilisateurs sont toujours à jour. Le délégué à la protection des données (DPD) devra bénéficier de capacités de reporting avancées dans différents domaines de la sécurité IT pour pouvoir s'assurer de la mise en conformité au titre du RGPD.

En outre, il devra pouvoir limiter l'envoi des documents contenant des données à caractère personnel en dehors de l'organisation afin de s'assurer que personne n'envoie par erreur des fichiers régis par le RGPD à des tiers non autorisés.

Certifications, codes de conduite et labels

Les organisations ont la possibilité d'adopter des mécanismes de certification aux fins de démontrer l'existence des garanties qu'ils appliquent. L'article 42 est un appel à l'action de la part des États membres, des autorités de contrôle et des autres institutions européennes, afin de mettre en place des mécanismes de certification de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement respectent le règlement. L'article 42 mentionne également un futur cadre de certification commun, le « label européen de protection des données », qui garantirait une norme de certification commune sur toute l'Union européenne, améliorant l'adoption et la clarté pour les citoyens.

Section 3 :

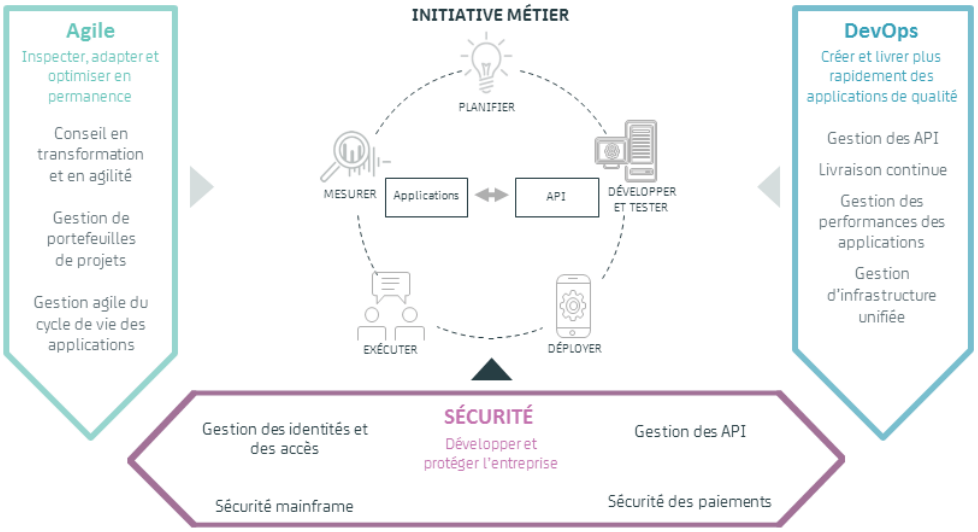
Que peut vous apporter CA Technologies ?

L'adhésion au règlement général de protection des données exigera une approche en profondeur, avec notamment l'assistance des départements juridique et IT, et dans certains cas, l'intervention de sociétés de conseil extérieures, afin de réaliser des études et des évaluations approfondies pour la réglementation elle-même, mais aussi une révision des processus organisationnels. En tant qu'éditeur de logiciels innovant et leader de l'économie des applications, CA Technologies guide les entreprises dans leur processus de transformation numérique et est à même de proposer toute une gamme de solutions logicielles pour les aider à remplir leurs obligations réglementaires.

CA Technologies offre aux entreprises les technologies dont elles ont besoin pour assurer la mise en conformité au titre du RGPD et déployer les contrôles qu'il impose, dans le but de mettre en place la philosophie globale de « sécurité dès la conception et par défaut », telle que préconisée par le règlement.

Ce qui différencie CA Technologies des fournisseurs de technologies spécialisées, c'est que nos solutions couvrent quasiment toutes les étapes du cycle de vie des données de l'organisation. Il est ainsi possible de combiner différentes solutions CA Technologies pour protéger l'accès aux données, gérer et contrôler les accès utilisateur, empêcher l'accès non autorisé aux données personnelles par des utilisateurs extérieurs ou internes, de façon à garantir le respect de la nouvelle réglementation en protégeant les droits des personnes concernées. CA Technologies dispose des outils et de l'expertise nécessaires pour guider les entreprises tout au long de ce processus complexe.

CA Technologies propose une stratégie DevOps globale et sécurisée, qui non seulement accélère le développement et la livraison des applications, mais garantit aussi la sécurité des applications et l'ensemble du cycle de livraison logicielle. Nos solutions de sécurité exhaustives incluent la gestion des API, la sécurité mainframe et une vaste gamme d'outils de gestion des accès et des identités (IAM). Pour en savoir plus sur nos solutions de sécurité IAM, visitez le site ca.com/iam.



CA Technologies et la classification et la localisation des données

Alors que les entreprises pensent savoir où les données à caractère personnel sont stockées et contrôlées, la réalité est toute autre ; ces données sont réparties sur l'ensemble de l'organisation et largement utilisées, transformées et récupérées de différentes manières et par différentes personnes. Les contrôles applicatifs ne sont donc pas suffisants pour garantir le respect de la nouvelle réglementation.

En outre, la précédente directive était davantage centrée sur la protection des fichiers contenant les données personnelles et le stockage des informations, alors que ce nouveau règlement cible plus spécialement le traitement des données. Cette nouvelle orientation est la conséquence de notre monde numérique actuel, où les données sont transformées, ajoutées, enrichies et traitées à très haute vitesse. Avec les outils d'analyse modernes fonctionnant sur le principe du Big Data, il est possible de combiner des éléments de données sans rapport entre eux afin de former des données à caractère personnel qui entrent dans le cadre de la nouvelle réglementation.

C'est pourquoi il est extrêmement important d'adopter une stratégie de défense approfondie en matière de protection des données à caractère personnel, de façon à leur appliquer plusieurs couches de contrôle.

Commençons par l'identification et la classification des données, de manière à déterminer où se situent les données à caractère personnel au sein de notre infrastructure. Si les données personnelles circulent en dehors des canaux et des flux prévus, il est important de comprendre ce phénomène et d'évaluer le risque associé.

Comprendre où résident les données à caractère personnel et qui y a accès au sein de l'organisation est l'un des principes fondamentaux du RGPD.

CA Data Content Discovery

Dans l'économie des applications, le système mainframe est de plus en plus connecté au reste du data center, et donc plus accessible aux utilisateurs lambda et soumis aux réglementations en matière de protection des données. Les ensembles de données sont copiés depuis la production, aux fins de développement ou de test, puis abandonnés ; d'autres restent orphelins lorsque leur propriétaire quitte l'entreprise. De plus, l'injection par les utilisateurs de données non structurées via les services système UNIX® peut laisser d'importants volumes de données sensibles ou réglementées masqués sur le mainframe, représentant un risque financier et d'atteinte à la réputation pour l'entreprise si ces données échappent à son contrôle.

Le mainframe héberge encore plus de 70 % des données critiques. Par exemple, si vous avez utilisé votre carte bancaire, réservé un billet d'avion ou passé un appel téléphonique aujourd'hui, il y a de grandes chances pour que vous soyez entré en contact avec un système mainframe. Toutefois, l'économie des applications a engendré de nouveaux risques pour le mainframe, car celui-ci est interconnecté avec la grande majorité des applications, et les violations de données font fréquemment les gros titres. Il serait catastrophique pour une entreprise que le mainframe et les données sensibles ou réglementées qu'il héberge soient touchés par une attaque.

Dans le monde IT hybride actuel, il n'est malheureusement pas toujours simple de déterminer, au sein des systèmes, quelles sont les données régies par la nouvelle réglementation. Pour y parvenir d'une façon adéquate et systématique, **CA Data Content Discovery** recherche, classifie et protège les données mainframe sensibles afin de couvrir le spectre complet des plates-formes existantes. Cette solution comprend des règles prédéfinies relatives aux données à caractère personnel, de manière non seulement à faciliter l'identification des informations, mais également à contrôler et suivre l'utilisation qu'en font les utilisateurs, tel que l'imposent divers articles du RGPD. L'analyse s'effectue à 100 % sur la plate-forme mainframe, afin que vos données ne soient pas dupliquées hors plate-forme. Cela permet aux organisations d'identifier et de protéger rapidement les données avant qu'une violation ne survienne.

CA Identity Suite

L'article 25, paragraphe 2, du RGPD stipule que « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. » L'article 30 impose quant à lui la tenue d'un registre des activités de traitement. Cela signifie que vous devez mettre en œuvre une solution capable de gérer et de gouverner l'accès des employés aux données à caractère personnel, de façon à réduire toute exposition inutile de ces données.

CA Identity Suite vous aide à gérer et à gouverner l'accès des utilisateurs aux applications métier et à leurs données sous-jacentes. La solution favorise le respect de cette exigence réglementaire, car elle génère des rapports indiquant qui a accès à quoi, et peut exécuter et gérer des campagnes de certification d'accès afin d'aider l'organisation dans ses efforts de mise en conformité.

Une approche courante permettant de respecter la conformité réglementaire consiste à valider régulièrement l'accès approprié des utilisateurs aux ressources de l'entreprise. Lors de la certification des accès, les responsables doivent passer en revue les listes des droits de leurs subordonnés directs et confirmer ou rejeter la légitimité des différents accès.

Avec CA Identity Suite, ce processus est simple et intuitif. Il permet ainsi d'accroître la productivité et la satisfaction des utilisateurs. Adapter un processus de certification aux besoins spécifiques d'une organisation est essentiel pour valider efficacement l'accès et encourager la participation au processus. CA Identity Suite peut solliciter une analyse sous plusieurs points de vue, par exemple celui des gestionnaires d'utilisateurs, des propriétaires de ressources ou des ingénieurs des rôles. Des processus de certification, appelés campagnes, peuvent être exécutés pour chacun de ces points de vue en utilisant

différents calendriers, workflows et approbateurs. En outre, plusieurs campagnes peuvent être menées simultanément, chacune visant différentes parties de l'organisation (par exemple, les utilisateurs d'une business unit donnée) ou mettant en évidence différents types d'accès (par exemple, uniquement les affectations suspectes ou les accès obtenus en dehors du modèle de rôle). CA Identity Suite inclut des contrôles et des workflows administratifs solides qui permettent d'assurer la progression des campagnes en fonction des besoins. Cette solution comprend notamment des notifications par courriel, des alertes de rappel et des processus d'escalade pour l'approbation des requêtes par des responsables de plus haut niveau. En outre, en cas de divergence et si des droits d'accès sont nécessaires, des processus de correction peuvent être déclenchés en affectant des tickets de correction aux propriétaires adéquats ou par le biais de l'intégration avec CA Identity Manager.

Dans le cadre du RGPD, les organisations doivent nommer une personne à un poste clé, celui de délégué à la protection des données (DPD). Dans ce rôle, les solutions technologiques visant à appuyer et démontrer l'ensemble des contrôles de sécurité que l'organisation a mis en place pour protéger les données à caractère personnel sont cruciales. Les fonctionnalités de reporting des solutions CA Technologies aident le DPD à prouver la conformité de l'organisation vis-à-vis du règlement RGPD, et sont utiles pour mettre en place les « analyses d'impact relatives à la protection des données » définies dans l'art. 35.

CA Identity Suite propose également des outils d'analyse intégrés qui fournissent des informations détaillées et facilement exploitables mettant en avant le fonctionnement des principaux processus d'identité (comme l'intégration des nouveaux utilisateurs). Ces outils d'analyse permettent d'identifier et de corriger les goulets d'étranglement et de respecter les engagements pris dans le cadre des accords sur les niveaux de service (SLA). CA Identity Governance inclut de nombreux rapports et tableaux de bord prêts à l'emploi et supporte les requêtes ad hoc pour les demandes externes. Les rapports varient selon le niveau d'informations métier et techniques fourni, pour répondre aux besoins des différents types d'utilisateurs. Il s'agit notamment de rapports distincts pour les chefs d'entreprise, les ingénieurs des rôles, les responsables de la mise en conformité, les auditeurs et le personnel IT, par exemple.

CA Test Data Manager

Les implications de la réglementation sont larges en ce qui concerne le type de données pouvant être utilisé dans les environnements hors production. Les organisations devront ainsi savoir exactement quelles données elles possèdent et qui les utilise, mais aussi être capables de limiter leur utilisation aux seules tâches pour lesquelles un consentement a été donné. L'une des façons d'éviter l'exposition des données à caractère personnel dans les environnements de test est tout simplement de ne pas les provisionner, même sous forme masquée. La génération de données synthétiques est une technique intéressante pour permettre aux organisations de passer à des environnements de test entièrement virtualisés.

Lors du test et du développement de logiciels, les données peuvent se retrouver dispersées entre les environnements de test et de développement, mais également dans d'autres environnements plus complexes. Il arrive, par exemple, que les testeurs copient les données dans leur environnement pour un usage donné, mais l'organisation doit désormais savoir combien de temps ces données seront utilisées et qu'elles le sont dans un but légitime, avec le consentement de la personne concernée. Effectuer un profilage des données dans **CA Test Data Manager** peut aider sur ce point en particulier, en identifiant exactement où les données sensibles sont stockées à l'échelle de l'entreprise, et en utilisant une analyse statistique pour rechercher les données à caractère personnel stockées dans différents formats de fichier et applications. En utilisant une vue cubique pour visualiser de façon exacte les données, CA Test Data Manager identifie les informations sensibles reflétées dans les systèmes, composants ou applications liés. Des filtres mathématiques personnalisés permettent de filtrer les données avec plus de détail, afin d'identifier chaque instance des informations pour un individu donné. Ces données peuvent inclure les numéros de carte de crédit, les adresses électroniques, les adresses postales, etc., ce qui aide les entreprises à satisfaire aux obligations relatives au droit de portabilité des données des personnes concernées. La fonction de détection des données proposée par CA Test Data Manager est entièrement auditable, de façon à ce que les entreprises puissent prouver les contrôles appliqués aux fins de mise en conformité.

CA API Management

Pour que les applications existantes qui intègrent des données à caractère personnel puissent devenir compatibles avec cette nouvelle réglementation, tout en évitant le coût élevé lié à des modifications, une seule réponse s'impose : les API.

La suite **CA API Management** permet aux entreprises de relever plus facilement les défis du partage des informations dans l'économie des applications. Cette solution combine des fonctionnalités avancées d'intégration back-end, d'optimisation mobile, d'orchestration Cloud et de gestion des développeurs, ainsi qu'une capacité unique lui permettant de prendre en charge l'ensemble des exigences de gestion des API des entreprises. Grâce à CA API Management, les entreprises peuvent prouver la mise en conformité de leurs systèmes avec la nouvelle réglementation, sans avoir à modifier leurs applications existantes. Elles peuvent en outre utiliser **CA Live API Creator** pour concevoir de nouvelles API intégrant les contrôles appropriés et exposant les informations nécessaires aux tierces parties.

Par exemple, en utilisant les solutions CA API Management, il est possible d'éviter la modification des applications existantes, une opération risquée et onéreuse, et de contrôler les comportements à l'aide d'une solution basée sur des règles et des politiques. L'organisation peut ainsi intégrer ses règles d'obtention de consentement et indiquer aux utilisateurs les informations requises au titre des articles 15 et 20 en documentant la méthode d'accès aux données via **CA API Developer Portal**. Ces contrôles de sécurité des accès sont fournis par la solution **CA API Gateway**.

Pour comprendre les avantages de cette approche, vous pouvez calculer le coût de la modification de l'ensemble des applications gérant actuellement des données personnelles au sein de votre organisation, et le comparer au coût d'une interface unique et normalisée, qui peut également servir à la mise en conformité pour d'autres réglementations sectorielles.

CA Privileged Access Manager

Qu'ils aient été obtenus de façon frauduleuse ou mal employés par un utilisateur légitime, l'exploitation des comptes d'utilisateurs à forts privilèges est le fil rouge de la majorité des violations de données. De plus, la complexité du système de défense pour contrecarrer des attaques toujours plus sophistiquées et préjudiciables s'accroît avec la complexité de votre environnement. CA Privileged Access Management est une suite complète de solutions qui met à votre disposition des contrôles basés sur le réseau et sur un hôte pour le Cloud d'entreprise et le Cloud hybride.

Bien que les entreprises soient tentées de croire que des contrôles d'accès basés sur les applications soient suffisants pour protéger l'accès aux données, la réalité est toute autre. En effet, la majorité des violations de données découlent de l'utilisation frauduleuse de comptes d'utilisateurs à forts privilèges, qui peuvent donc sans problème contourner les contrôles d'accès en place, ce qui les rend inutiles. C'est pourquoi les entreprises doivent mettre en place des contrôles de sécurité servant à la fois à gérer et à gouverner les accès à forts privilèges.

CA Privileged Access Manager (CA PAM) est une solution éprouvée et facile à déployer, qui permet une gestion des accès à forts privilèges dans les environnements physiques, virtuels et Cloud de l'organisation. Disponible sous forme d'appliance matérielle renforcée montée sur rack, d'appliance virtuelle OVA (Open Virtual Appliance) ou d'instance AMI (Amazon Machine Instance), CA PAM renforce la sécurité en assurant la protection des identifiants administratifs sensibles, en contrôlant l'accès des utilisateurs à forts privilèges, en appliquant les règles de sécurité de manière proactive et en supervisant et enregistrant l'activité des utilisateurs à forts privilèges sur l'ensemble des ressources IT.

CA Privileged Access Manager Server Control, l'un des composants de CA PAM, offre quant à lui une protection complète pour vos serveurs critiques grâce à des contrôles fins et puissants appliqués aux accès de niveau système et aux actions des utilisateurs à forts privilèges. Capable de mettre en œuvre des contrôles d'accès sur les puissants comptes de superutilisateur natifs (tels que les comptes root UNIX et Linux® et les comptes d'administrateur Microsoft® Windows®), cette solution système, basée sur un hôte, permet de contrôler, de superviser et d'auditer l'activité des utilisateurs à forts privilèges, ce qui renforce la sécurité et simplifie les missions d'audit et de mise en conformité.

En combinant CA Privileged Access Manager Server Control, pour le renforcement des serveurs, et CA Privileged Access Management, vous obtenez la solution la plus complète possible pour gérer les accès et les utilisateurs à forts privilèges de votre organisation.

CA Single Sign-On

L'économie des applications a modifié les interactions entre les entreprises et leurs clients. Les utilisateurs exigent aujourd'hui de pouvoir accéder aux services et données en ligne à tout moment, où qu'ils se trouvent, et s'attendent à une expérience utilisateur transparente et unifiée, quels que soient les équipements et les canaux utilisés. Dans le cadre du RGPD, les organisations doivent trouver le juste équilibre entre la simplicité de l'accès et les données auxquelles il est possible d'accéder. Comment faire pour s'assurer que seules les personnes habilitées auront accès au contenu sensible, et ce uniquement au moment où la loi l'autorise ? Par exemple, un citoyen européen a le droit de consulter ses données personnelles. Mais a-t-il le droit d'y accéder et de les consulter s'il se connecte depuis un pays autre que les États-Unis ? Qu'en est-il des employés d'une entreprise ? Peut-être peuvent-ils accéder à ces mêmes données lorsqu'ils se connectent depuis les États-Unis, mais pas depuis un autre pays ?

CA Single Sign-On permet de faire face à ce type de problématique en offrant aux employés, clients, partenaires et fournisseurs un accès par authentification unique (SSO, Single Sign-On) aux applications en ligne, où qu'ils se trouvent dans le monde, quel que soit le type d'appareil utilisé pour y accéder et indépendamment du mode d'authentification (connexion directe, via les réseaux sociaux ou en fédération depuis un site partenaire). Cette solution renforce également la sécurité en instaurant une couche de règles communes qui réduit les lacunes éventuelles entre les diverses règles d'accès.

Le RGPD impose aux organisations d'octroyer aux utilisateurs l'accès aux données personnelles, mais aussi de limiter le nombre de personnes pouvant y accéder. Une solution complète de gestion des accès telle que CA Single Sign-On peut offrir les contrôles d'accès Web appropriés pour ces deux types d'utilisateur, depuis un point centralisé. Externaliser cet élément de sécurité par rapport aux applications elles-mêmes va dans le sens d'une sécurité « dès la conception », dans l'approche DevSecOps.

CA Directory

Le RGPD implique une refonte majeure de la législation existante en matière de protection des données, et bien que la majorité de ces données soit hébergée sur les mainframes des grandes entreprises, une part importante est également stockée dans les annuaires. Les entreprises d'aujourd'hui se reposent de plus en plus sur les applications mobiles et en ligne pour fournir les services critiques à leurs utilisateurs. Elles rencontrent toutefois des problèmes de performances et de disponibilité dus à l'infrastructure d'annuaires sous-jacentes, notamment les suivants :

- **Croissance explosive :** l'explosion du nombre d'identités utilisateur et d'équipements, et la fonctionnalité de maintenance de la réactivité nécessaire pour offrir une expérience utilisateur de qualité constituent un vrai casse-tête pour nombre de référentiels existants.
- **Silos d'identités :** de nombreux annuaires ont été déployés par différentes business units au fil du temps, et ils engendrent aujourd'hui des problèmes, entre autres une expérience utilisateur médiocre, des risques de sécurité et des coûts opérationnels en hausse.
- **Nouvelles exigences :** les exigences en matière de sécurité évoluent, allant de la simple authentification utilisateur au suivi détaillé des données de session et des informations personnalisées associées aux opérations métier dynamiques.

En conséquence, de nombreux clients souhaitent améliorer leur infrastructure de gestion des identités et des accès (IAM), et migrent vers un service d'annuaire nouvelle génération offrant de meilleures performances pour un coût de possession moindre. Cependant, le RGPD apporte également une nouvelle variable en matière de critères d'évaluation. Votre service d'annuaire nouvelle génération doit avoir la capacité à partitionner l'arborescence des répertoires sur de multiples serveurs, permettant à l'organisation de savoir où sont physiquement stockées les données à caractère personnel. Il doit en outre vous permettre de déterminer de façon sélective quelles sont les données répliquées sur les différents nœuds, afin d'empêcher ces données de quitter une région spécifique.

CA Cleanup

CA Cleanup identifie les comptes inutilisés au-delà du seuil défini et génère des commandes pour supprimer les ID d'utilisateur, les droits, les autorisations, ainsi que les profils et les connexions de groupe dont chaque utilisateur dispose, mais qu'il n'utilise pas. Cette solution permet de résoudre efficacement le problème de l'accumulation progressive de droits d'accès obsolètes et excessifs dans un fichier de sécurité, ce qui est d'ailleurs imposé par de nombreuses réglementations. CA Cleanup se déploie entièrement en une seule journée et offre les fonctionnalités suivantes :

- Identification et suppression des utilisateurs, droits et groupes d'accès devenus inutiles.
- Identification des droits (autorisations et règles) réellement utilisés et création de commandes pour supprimer ceux qui ne le sont plus, Y compris les ressources définies par l'utilisateur.
- Identification des ID utilisateur réellement utilisés et création de commandes pour supprimer ceux qui ne le sont plus. Cette fonction est basée sur l'utilisation de sécurité réelle, et non sur les dates de dernière utilisation, souvent peu fiables.
- Génération de rapports sur les droits utilisés et non utilisés.
- Génération de commandes pour activer ou restaurer le nettoyage de sécurité.

En combinant CA Cleanup et CA ACF2™, vous pouvez distinguer les ID de connexion, les règles et les ensembles de règles actifs de ceux qui ne le sont pas, y compris les classes de ressource personnalisées et les règles NEXTKEY sources et cibles. En combinant CA Cleanup et CA Top Secret®, vous pouvez déterminer les ID d'accès, les autorisations et les profils actifs de ceux qui ne le sont pas, et ce y compris pour les ressources définies par l'utilisateur et l'enregistrement *ALL*. En combinant CA Cleanup et IBM® RACF®, vous pouvez distinguer les ID d'utilisateur, les profils, les autorisations, les connexions de groupe et les groupes de ressources IBM RACF actifs de ceux qui ne le sont pas. Vous effectuez un suivi de l'utilisation des autorisations pour chaque entrée de liste d'accès donnée, qu'elle soit isolée, générique ou conditionnelle.

CA Compliance Event Manager

CA Compliance Event Manager permet de superviser de façon proactive la sécurité, tout en aidant à réduire les coûts, la complexité et le travail nécessaires à la supervision et au reporting en matière de sécurité et de conformité mainframe. Grâce à différents composants conçus pour traiter les informations relatives aux événements du gestionnaire de sécurité externe et superviser en toute transparence les systèmes, de manière à détecter toute modification des ressources critiques, CA Compliance Event Manager alerte, inspecte et protège les données de mainframe critiques afin d'offrir aux parties prenantes des notifications en temps réel sur les potentielles violations de sécurité.

Une part importante de la mise en conformité dans le cadre du RGPD portera sur la façon dont les données seront recueillies à l'avenir. Mais cela concerne aussi toutes les données que les entreprises détiennent déjà. Nombre de systèmes mainframe hébergent des données présentes depuis des générations. Dans un tel cas, un audit manuel est hors de question. C'est là que CA Compliance Event Manager entre en scène, en proposant trois fonctionnalités essentielles :

- **Alerte :** cette solution supervise l'ensemble des systèmes des enregistrements de sécurité, les points de configuration de sécurité, les ensembles de données système et les contrôles de configuration IBM z/OS®, grâce à une notification immédiate et en temps réel des violations, activités d'accès et de modification pertinentes détectées sur les ressources et les systèmes de sécurité critiques. Les parties prenantes bénéficient ainsi d'informations immédiates et pertinentes sur le potentiel et l'ampleur de l'exposition de données sur le mainframe, de façon à pouvoir prévenir de manière proactive les événements de sécurité indésirables.
- **Inspection :** une fois les menaces d'exposition de données identifiées, CA Compliance Event Manager génère des informations d'audit et de conformité avancées, qui ne sont pas disponibles dans les rapports de sécurité standard. Grâce à un processus sophistiqué de collecte des données, d'audit complet et d'entreposage des données, la solution permet aux utilisateurs de relire tous les événements de sécurité aux fins d'analyse, d'étudier a posteriori les enregistrements de données de sécurité brutes et de consulter, de filtrer et d'analyser les données d'historique enregistrées grâce à une récupération automatique des bandes, dans le but de mieux comprendre les problèmes de conformité et de sécurité et d'améliorer le profil de risque.
- **Protection :** après avoir reçu des notifications en temps réel et inspecté les expositions de données pour effectuer un triage rapide des problèmes, vous bénéficiez d'un meilleur contrôle sur vos données mainframe et êtes mieux préparé pour savoir qui a accès aux données régies par le RGPD (employés, clients et partenaires commerciaux, passés et présents), de façon à vous assurer que les autorisations adéquates sont appliquées.

Section 4 :

Conclusion

La mise en conformité au titre du règlement général sur la protection des données (RGPD) peut se faire par une combinaison de personnes, de processus et de technologies. Le présent document vous a décrit les solutions qui peuvent aider les entreprises à réussir leur parcours RGPD. Vous avez toutefois la possibilité d'étendre cette protection et de renforcer encore davantage vos contrôles de sécurité, grâce à une authentification forte et basée sur les risques ou à une automatisation de la charge de travail pour automatiser le traitement des données à caractère personnel, de façon à garantir le respect du RGPD, mais aussi des obligations réglementaires autres. Les réglementations établissent généralement des normes minimales à respecter, mais dans l'économie des applications, les entreprises ouvertes doivent faire tout ce qui est en leur pouvoir pour protéger la plus importante et la plus précieuse de leurs ressources : les données privées des clients.

Il est donc important de ne pas envisager le RGPD comme un règlement isolé, mais de l'appréhender dans le contexte des autres lois et réglementations existantes, y compris celles qui sont spécifiques au secteur, et qui visent à protéger les données dans l'économie des applications. Des contrôles solides pour assurer la sécurité et la protection des données, et gérer la façon dont les personnes les utilisent et y accèdent, sont essentiels pour les entreprises qui souhaitent se conformer à ces lois et réglementations, quel que soit leur secteur d'activité.

Consultez ces ressources pour en savoir plus sur les solutions CA Technologies et le RGPD :

- eBook : « Complying with the EU General Data Protection Regulation. The Implications for Test Data Management »
- Livre blanc : « EU General Data Protection Regulation (GDPR): Are you ready for it? »

Restez connecté à CA Technologies sur ca.com/fr

CA Technologies (NASDAQ : CA) fournit les logiciels qui aident les entreprises à opérer leur transformation numérique. Dans tous les secteurs, les modèles économiques des entreprises sont redéfinis par les applications. Partout, une application sert d'interface entre une entreprise et un utilisateur. CA Technologies aide ces entreprises à saisir les opportunités créées par cette révolution numérique et à naviguer dans « l'Économie des applications ». Grâce à ses logiciels pour planifier, développer, gérer les performances et la sécurité des applications, CA Technologies aide ainsi ces entreprises à devenir plus productives, à offrir une meilleure qualité d'expérience à leurs utilisateurs et leur ouvre de nouveaux relais de croissance et de compétitivité sur tous les environnements : mobile, Cloud, distribué ou mainframe. Pour plus d'informations, rendez-vous sur le site ca.com/fr.

CS200-255926_0217